REMARKS

Applicant's invention relates to a two-step method for generating certified time stamp receipts for digital documents. In the first stage, identifying data, such as a hash of the document, is presented to a time stamping authority. The time stamping authority appends a time stamp to the identifying data to create an uncertified time stamp receipt. Additionally, the time stamping authority generates a message authentication code based on the uncertified time stamp receipt and a secret key. The uncertified time stamp receipt and the message authentication code are transmitted to the requestor.

In the second stage, either the original requestor or other third party may request certification of the time stamp receipt. The requestor or other third party presents the uncertified time stamp receipt and the message authentication code to the time stamping authority. The time stamping authority validates the message authentication code and, if the message authentication code is valid, certifies the time stamp receipt using a private signature key.

The prior art cited by the Examiner does not teach or suggest the two-stage certification process set forth in the claims. The Haber patent discloses a conventional time stamping process wherein the time stamping authority appends a time stamp to identifying data received from the requestor and immediately certifies the time stamp receipt by signing the time stamp receipt with a private signature key. Haber does not teach or suggest either the two-step process recited in the claims, or the use of message authentication codes.

The Examiner acknowledges that Haber fails to teach generating a message authentication code, but recites Bruce Schneier's book entitled *Applied Cryptography* to show that message authentication codes are well known. The Examiner then recites numerous advantages to using a message authentication code to improve the security of a time stamping procedure and concludes that the invention would be obvious. The Examiner's analysis is conducted only at a high level of generality and glosses over important limitations of the claimed inventions.

First, the mere fact that message authentication codes are well known does not mean that use of message authentication codes for the purposes cited in the claim is known or that the manner in which the message authentication codes recited in the claim are known. The Examiner cites no references showing use of message authentication codes in time stamping procedures.

Second, the Examiner's enumeration of the advantages of using message authentication codes is not something that the Examiner derived from the prior art but, instead, are advantages that the Examiner gleaned only after the Examiner reviewed Applicant's application. Again, there is nothing in the prior art to suggest the advantages gained by incorporating message authentication codes into time stamping procedures. The Examiner's entire analysis is based on hindsight.

Finally, even assuming that there were some suggestions in the prior art to use message authentication codes in a time stamping procedure, there is still nothing in the prior art to suggest the particular manner of using the message authentication codes set forth in the claims. The mere fact that message authentication codes may be used in a time stamping procedure does not suggest the two-stage process recited in the claims. As noted above, an uncertified time stamp receipt and message authentication code are generated during a first stage. In the second stage, which occurs at a different point in time, a person may present the time stamp receipt and message authentication code to the time stamping authority to request certification of the time stamp receipt. The time stamping authority verifies the message authentication code and certifies the time stamping receipt only if the message authentication code is valid. None of the references cited by the Examiner suggest this two-stage process for generating time stamp receipts.

Claims 1 and 15 both require that a time stamp request and a certification request be presented to the time stamping authority at two distinct times. Claims 1 and 15 require generating a message authentication code at a first time and certifying the time stamp receipt at

a second time only if the message authentication code is valid. The prior art does not teach or suggest the claimed two-step process. The Examiner fails to address the two-step feature in his arguments, or to cite any references suggesting a two-step time stamping procedure. Accordingly, claims 1 and 15 are allowable over the art cited by the Examiner.

Claim 29 is a method claim directed to the first stage of the certification process. Claim 29 recites generating a message authentication code based on a time stamp receipt and a secret key, and transmitting the uncertified time stamp receipt and message authentication code to a requestor. Claim 41 recites acts associated with the second stage of the certification process. Claim 41 recites receiving a certification request, including a time stamp receipt and a message authentication code generated on the time stamp receipt, validating the message authentication code and certifying the time stamp receipt if the message authentication code is valid. Again, the prior art does not teach or suggest the two-stage process or the particular manner in which the message authentication code is used in a two-step process as recited in claims 29 and 41. Accordingly, it is believed that claims 29 and 41 are allowable.

Based on the foregoing, it is believed that the present application is in condition for allowance and notice to such effect is respectfully requested.

Respectfully submitted,

COATS & BENNETT, P.L.L.C.

By: David E. Bennett

David E. Bennett
Registration No. 32,194

P.O. Box 5
Raleigh, NC 27602
Telephone: (919) 854-1844